PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-107536
(43)Date of publication of application : 22.04.1997

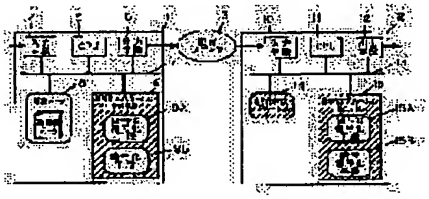
(51)Int.Cl. H04N 7/167
G09C 1/00
G09C 1/00
H04K 1/06
H04L 9/14
H04L 9/34

(21)Application number : 07-261242
(22)Date of filing : 09.10.1995

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HARADA TOSHIHARU
TATEBAYASHI MAKOTO
MATSUZAKI NATSUME
KOZUKA MASAYUKI
YAMAUCHI KAZUHIKO

(54) DATA CIPHERING DEVICE AND SYSTEM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data ciphering system by which processing cost is reduced for ciphering processing with respect to an application processing data requesting real time processing such as dynamic image data and sufficient security is secured under the limitation of real time processing and to provide the device therefor.
SOLUTION: This data ciphering system is made up of a device A1 generating a ciphered application used by a software server and a device B2 decoding and reproduction the ciphered application used by the software user. The device A1 has a CPU 5 controlling the entire operation and it is connected to object data 8, a ciphering application generating means 9, an input means 4, an output means 5 by a bus 7. The device B2 has a CPU 11 controlling the entire operation and it is connected to a ciphered application 14 received from a distributed medium 3, ciphered application reproduction means 15, an input means 10 and an output means 12 via a bus 13.



LEGAL STATUS

[Date of request for examination] 07.06.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－107536

(43)公開日　平成９年(1997)４月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｎ	7/167			Ｈ０４Ｎ	7/167	
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ａ
		６６０	7259－5Ｊ			６６０Ｚ
Ｈ０４Ｋ	1/06			Ｈ０４Ｋ	1/06	
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６４１

審査請求　未請求　請求項の数34　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平7－261242

(22)出願日　平成７年(1995)10月９日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外１名）

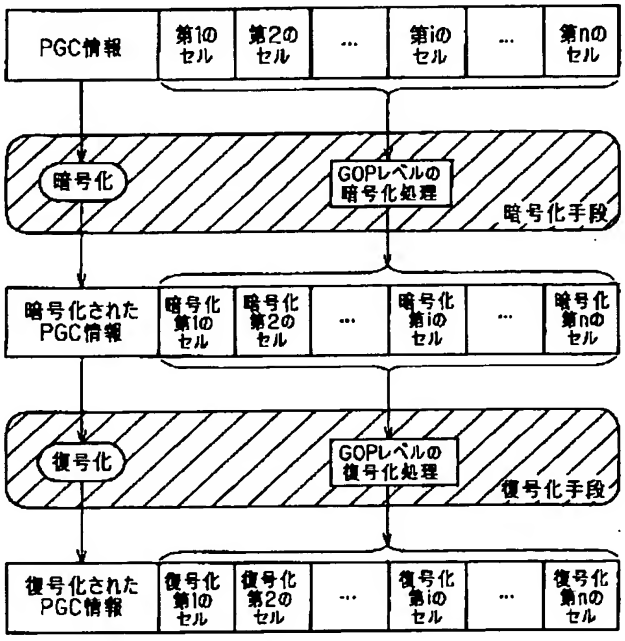
最終頁に続く

(54)【発明の名称】　データ暗号方式及びデータ暗号システム

(57)【要約】

【課題】　実時間処理の要求されるデータを扱うアプリケーションに対し、実時間処理の制約の中で十分な機密性を確保できるデータ暗号方式および装置を提供する。

【解決手段】　暗号化対象とするアプリケーションは１個以上セルと、各セルの再生順序を記述したＰＧＣ情報より構成する。暗号化処理はこのＰＧＣ情報の暗号化処理とＧＯＰレベルの暗号化処理、すなわちビデオデータの再生制御の単位であるＧＯＰ毎に付加される早送り再生や巻き戻し再生時の飛び先情報を記述したＤＳＩ情報の暗号化と再生順序とは無関係な順序で各ＧＯＰをインタリーブする。復号化処理は暗号化されたＰＧＣ情報の復号化処理とＧＯＰレベルの復号化処理、すなわち暗号化されたＤＳＩ情報の復号化を行う。



【特許請求の範囲】

【請求項１】再生順序の規定された複数の再生データの連なりから構成される対象データに対して、機密性保持処理を施すデータ暗号方式であって、

前記各再生データの再生順序を規定する再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化する暗号化ステップと、

前記再生順序制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生順序制御情報に基づいて再生すべき再生データを決定する、復号化ステップとを有することを特徴とするデータ暗号方式。

【請求項２】再生順序の規定された複数の再生データの連なりから構成される対象データに対して、機密性保持処理を施すデータ暗号方式であって、

前記各再生データ毎に保持され、次に再生すべき再生データを規定する再生制御情報の一部または全部を暗号化鍵を用いて暗号化する暗号化ステップと、

前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生制御情報に基づいて次に再生すべき再生データを決定する、復号化ステップとを有することを特徴とするデータ暗号方式。

【請求項３】再生順序の規定された複数の再生データの連なりから構成される対象データに対して、機密性保持処理を施すデータ暗号方式であって、

前記対象データが、再生順序の規定された複数の再生データ群の連なりから構成され、さらに各再生データ群がそれぞれ再生データ群内において再生順序の規定された複数の再生データの連なりから構成される場合に、

前記各再生データ群の再生順序を規定する再生順序制御情報と、前記各再生データ毎に保持され、次に再生すべき再生データを規定する再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化する暗号化ステップと、

前記再生順序制御情報と前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生順序制御情報に基づいて再生すべき再生データ群を決定し、復号化された再生制御情報に基づいて再生すべき再生データを決定し、決定された再生データを再生する復号化ステップとを有することを特徴とするデータ暗号方式。

【請求項４】前記暗号化ステップは、前記再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化し、さらに各再生データを前記再生順序とは無関係な順序に配置して複数の再生データの連なりとするようにしたことを特徴とする請求項１記載のデータ暗号方式。

【請求項５】前記暗号化ステップは前記再生制御情報の一部または全部を暗号化鍵を用いて暗号化し、さらに各再生データを前記再生順序とは無関係な順序に配置して複数の再生データの連なりとするようにしたことを特徴とする請求項２記載のデータ暗号方式。

【請求項６】前記暗号化ステップは前記再生順序制御情報と、前記再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化し、さらに前記各再生データ、前記各再生データ群、または前記各再生データと前記各再生データ群を前記再生順序とは無関係な順序に配置して複数の再生データの連なりとするようにしたことを特徴とする請求項３記載のデータ暗号方式。

【請求項７】前記暗号化ステップは前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化するようにし、

前記復号化ステップは、暗号化された前記システムストリーム再生順序制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記システムストリーム再生順序制御情報にしたがって再生すべきシステムストリームを決定するようにしたことを特徴とする請求項１記載のデータ暗号方式。

【請求項８】前記暗号化ステップは前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリームのGOP 毎に保持され、次に再生するGOP を規定する再生制御情報の一部または全部を暗号化鍵を用いて暗号化するようにし、

前記復号化ステップは暗号化された前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記再生制御情報にしたがって、再生すべきGOP を決定するようにしたことを特徴とする請求項２記載のデータ暗号方式。

【請求項９】前記暗号化ステップは前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に前記圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報と、前記圧縮された動画像データのシステムストリームのGOP 毎に保持され、次に再生するGOP を規定する再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化するようにし、

前記復号化ステップは、暗号化された前記システムストリーム再生順序制御情報と、暗号化された前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記システムストリーム再生順序制御情報にしたがって再生すべきシステムストリームを決定し、復号化された前記再生制御情報にしたがって再生すべきGOP を決定するようにしたことを特徴とする請求項３記載のデータ暗号方式。

【請求項１０】前記暗号化ステップは前記システムストリーム再生順序制御情報の一部または全部を暗号化鍵を

用いて暗号化し、前記各システムストリーム群を再生順序とは無関係な順序に配置するようにしたことを特徴とする請求項７記載のデータ暗号方式。

【請求項１１】前記暗号化ステップは前記再生制御情報の一部または全部を暗号化鍵を用いて暗号化し、前記各GOPを再生順序とは無関係な順序に配置するようにしたことを特徴とする請求項８記載のデータ暗号方式。

【請求項１２】前記暗号化ステップは前記システムストリーム再生順序制御情報と、前記再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化し、前記各GOP、または前記各システムストリーム群、または前記各GOPとシステムストリーム群を再生順序とは無関係な順序に配置するようにしたことを特徴とする請求項９記載のデータ暗号方式。

【請求項１３】前記暗号化ステップに各再生データ間に無意味なデータを配置するステップを追加したことを特徴とする請求項１から１２のいずれか１項に記載のデータ暗号方式。

【請求項１４】前記暗号化ステップは、前記対象データの一部または全部をも前記暗号化鍵を用いて暗号化するようにし、

前記復号化ステップは前記暗号化された部分をも前記暗号化鍵に対応する復号化鍵を用いて復号化するようにしたことを特徴とする請求項１から１２のいずれか１項に記載のデータ暗号方式。

【請求項１５】それぞれデータ入力部より入力されたデータを鍵入力部より入力されたデータを用いて暗号化する第１の暗号アルゴリズム、及び第１の暗号アルゴリズムより高速な第２の暗号アルゴリズムと、

前記第１及び第２の暗号化アルゴリズムにそれぞれ対応して、データ入力部より入力されたデータを鍵入力部より入力されたデータを用いて復号化する第１、及び第２の暗号アルゴリズムとを用いて、

前記暗号化ステップにおける暗号化処理は、暗号化処理を施すデータを第１、第２、…、第ｎのデータブロックに分割し、

前記第１の暗号化アルゴリズムにしたがって、前記データ入力部より入力された前記第１のデータブロックを前記鍵入力部より入力された初期設定値と、暗号化鍵を用いて暗号化し、

前記第２の暗号化アルゴリズムにしたがって、前記データ入力部より入力された前記第ｉ（２≦ｉ≦ｎ）のデータブロックをそれぞれ前記鍵入力部より入力された前記第（ｉ－１）のデータブロックと、暗号化鍵を用いて暗号化するようにし、

前記復号化ステップにおける復号化処理は、前記第１の復号化アルゴリズムにしたがって前記データ入力部より入力された暗号化された前記第１のデータブロックを前記鍵入力部より入力された前記初期設定値と前記復号化鍵を用いて復号化し、

前記第２の復号化アルゴリズムにしたがって前記データ入力部より入力された、暗号化された前記第ｉのデータブロックを、前記鍵入力部により入力された前記第（ｉ－１）のデータブロックと、前記復号化鍵を用いて復号化し、復号化された前記第１、第２、…、第ｎのデータブロックを結合して前記データを復元するようにしたことを特徴とする請求項１から１２のいずれか１項に記載のデータ暗号方式。

【請求項１６】前記初期値に変えて暗号化された第ｊ（ｊは２≦ｊ≦ｎを満たす整数）のデータブロックを用いるようにしたことを特徴とする請求項１５記載のデータ暗号方式。

【請求項１７】前記第１の暗号化アルゴリズム及び復号化アルゴリズムは、それぞれ基本処理部をＭ回繰り返す構成とし、前記第２の暗号化アルゴリズム及び復号化アルゴリズムは前記基本処理部をｍ（＜Ｍ）回繰り返す構成とするようにしたことを特徴とする請求項１５記載のデータ暗号方式。

【請求項１８】再生順序の規定された複数の再生データの連なりから構成される対象データに対して機密性保持処理を施すデータ暗号システムであって、

前記各再生データの再生順序を規定する再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化する暗号化手段と、

前記再生順序制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生順序制御情報に基づいて再生すべき再生データを決定する復号化手段とを有することを特徴とするデータ暗号システム。

【請求項１９】再生順序の規定された複数の再生データの連なりから構成される対象データに対して、機密性保持処理を施すデータ暗号システムであって、

前記各再生データ毎に保持され、次に再生すべき再生データを規定する再生制御情報の一部または全部を暗号化鍵を用いて暗号化する暗号化手段と、

前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生制御情報に基づいて次に再生すべき再生データを決定する、復号化手段とを有することを特徴とするデータ暗号システム。

【請求項２０】再生順序の規定された複数の再生データの連なりから構成される対象データに対して、機密性保持処理を施すデータ暗号システムであって、

前記対象データが再生順序の規定された複数の再生データ群の連なりから構成され、さらに各再生データ群が、それぞれ再生データ群内において再生順序の規定された複数の再生データの連なりから構成される場合に、

前記各再生データ群の再生順序を規定する再生順序制御情報と、前記各再生データ毎に保持され、次に再生すべき再生データを規定する再生制御情報のそれぞれ一部ま

たは全部を暗号化鍵を用いて暗号化する暗号化手段と、前記再生順序制御情報と前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生順序制御情報に基づいて再生すべき再生データ群を決定し、復号化された再生制御情報に基づいて再生すべき再生データを決定し、決定された再生データを再生する復号化手段とを有することを特徴とするデータ暗号システム。

【請求項２１】前記暗号化手段は前記再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化し、さらに各再生データを前記再生順序とは無関係な順序に配置して複数の再生データの連なりとするようにしたことを特徴とする請求項１８記載のデータ暗号システム。

【請求項２２】前記暗号化手段は前記再生制御情報の一部または全部を暗号化鍵を用いて暗号化し、さらに各再生データを前記再生順序とは無関係な順序に配置して複数の再生データの連なりとするようにしたことを特徴とする請求項１９記載のデータ暗号システム。

【請求項２３】前記暗号化手段は前記再生順序制御情報と、前記再生制御情報と、のそれぞれ一部または全部を暗号化鍵を用いて暗号化し、さらに前記各再生データ、または前記各再生データ群、または前記各再生データと前記各再生データ群を前記再生順序とは無関係な順序に配置して複数の再生データの連なりとするようにしたことを特徴とする請求項２０記載のデータ暗号システム。

【請求項２４】前記暗号化手段は前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化するようにし、

前記復号化手段は、暗号化された前記システムストリーム再生順序制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記システムストリーム再生順序制御情報にしたがって、再生すべきシステムストリームを決定するようにしたことを特徴とする請求項１８記載のデータ暗号システム。

【請求項２５】前記暗号化手段は、前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリームのGOP 毎に保持され、次に再生するGOP を規定する再生制御情報の一部または全部を暗号化鍵を用いて暗号化するようにし、

前記復号化手段は、暗号化された前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記再生制御情報にしたがって再生すべきGOP を決定するようにしたことを特徴とする請求項１９記載のデータ暗号システム。

【請求項２６】前記暗号化手段は、前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報と、前記圧縮された動画像データのシステムストリームのGOP 毎に保持され、次に再生するGOP を規定する再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化するようにし、

前記復号化手段は、暗号化された前記システムストリーム再生順序制御情報と、暗号化された前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記システムストリーム再生順序制御情報にしたがって、再生すべきシステムストリームを決定し、復号化された前記再生制御情報にしたがって再生すべきGOP を決定するようにしたことを特徴とする請求項２０記載のデータ暗号システム。

【請求項２７】前記暗号化手段は前記システムストリーム再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化し、前記各システムストリーム群を、再生順序とは無関係な順序に配置するようにしたことを特徴とする請求項２４記載のデータ暗号システム。

【請求項２８】前記暗号化手段は前記再生制御情報の一部または全部を暗号化鍵を用いて暗号化し、前記各GOP を再生順序とは無関係な順序に配置するようにしたことを特徴とする請求項２５記載のデータ暗号システム。

【請求項２９】前記暗号化手段は前記システムストリーム再生順序制御情報と、前記再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化し、前記各GOP 、または前記各システムストリーム群、または前記各GOPとシステムストリーム群を再生順序とは無関係な順序に配置するようにしたことを特徴とする請求項２６記載のデータ暗号システム。

【請求項３０】前記暗号化手段に各再生データ間に無意味なデータを配置するステップを追加したことを特徴とする請求項１８から２９のいずれか１項に記載のデータ暗号システム。

【請求項３１】前記暗号化手段は前記対象データの一部または全部を前記暗号化鍵を用いて暗号化するようにし、

前記復号化手段は、前記暗号化された部分をも前記暗号化鍵に対応する復号化鍵を用いて復号化するようにしたことを特徴とする請求項１８から２９のいずれか１項に記載のデータ暗号システム。

【請求項３２】それぞれデータ入力部より入力されたデータを、鍵入力部より入力されたデータを用いて暗号化する第１の暗号アルゴリズム、及び第１の暗号アルゴリズムより高速な第２の暗号アルゴリズムと、

前記第１及び第２の暗号化アルゴリズムにそれぞれ対応して、データ入力部より入力されたデータを鍵入力部より入力されたデータを用いて復号化する第１、及び第２の暗号アルゴリズムとを用いて前記暗号化手段における

暗号化処理は、暗号化処理を施すデータを第１、第２、…、第ｎのデータブロックに分割し、
前記第１の暗号化アルゴリズムにしたがって前記データ入力部より入力された前記第１のデータブロックを前記鍵入力部より入力された初期設定値と、暗号化鍵を用いて暗号化し、
前記第２の暗号化アルゴリズムにしたがって、前記データ入力部より入力された前記第ｉ（２≦ｉ≦ｎ）のデータブロックをそれぞれ前記鍵入力部より入力された、前記第（ｉ－１）のデータブロックと暗号化鍵を用いて暗号化するようにし、
前記復号化手段における復号化処理は、前記第１の復号化アルゴリズムにしたがって、前記データ入力部より入力された暗号化された前記第１のデータブロックを前記鍵入力部より入力された、前記初期設定値と前記復号化鍵を用いて復号化し、
前記第２の復号化アルゴリズムにしたがって、前記データ入力部より入力された暗号化された、前記第ｉのデータブロックを前記鍵入力部により入力された前記第（ｉ－１）のデータブロックと前記復号化鍵を用いて復号化し、復号化された前記第１、第２、…、第ｎのデータブロックを結合して前記データを復元するようにしたことを特徴とする請求項１８から２９のいずれか１項に記載のデータ暗号システム。
【請求項３３】前記初期値に変えて暗号化された第ｊ（ｊは２≦ｊ≦ｎを満たす整数）のデータブロックを用いるようにしたことを特徴とする請求項３２記載のデータ暗号システム。
【請求項３４】前記第１の暗号化アルゴリズム及び復号化アルゴリズムはそれぞれ基本処理部をＭ回繰り返す構成とし、前記第２の暗号化アルゴリズム及び復号化アルゴリズムは、前記基本処理部をｍ（＜Ｍ）回繰り返す構成とするようにしたことを特徴とする請求項３２記載のデータ暗号システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】動画像データのように実時間処理の要求される対象データを扱うアプリケーションに対してスクランブル処理を施すデータ暗号方式及びデータ暗号システムに関する。
【０００２】
【従来の技術】従来、データの機密性を確保したり、あるいは、データに対する不正アクセスや、コピーの防止などのために、データを暗号化することが一般に行なわれている。
【０００３】例えば、UNIXワークステーションでは、データ機密性を確保するための手段として、ＤＥＳ（Data Encryption Standard:データ暗号化規格）などに代表される暗号化手段を提供している。そして、この暗号化手段を利用してファイルを暗号化することにより、その機密性を確保したり、不正アクセスやコピーの防止を図ることができる。
【０００４】
【発明が解決しようとする課題】しかしながら、上記従来例では動画像などの大量のデータの機密性を確保しようとすると、暗号化処理に時間がかかるため、暗号処理に要するコストが増えるだけでなく、アプリケーションに要求される実時間処理の制約の中で暗号処理を十分に行なえないという問題があった。
【０００５】例えば、動画像の暗号処理に、ソフトウエアインプリメントされたＤＥＳを利用する場合、暗号処理速度は320kbps（80286プロセッサ、25MHz）程度である。従って、一般に数Mbps以上の処理が要求される動画像データに対しては、暗号処理がオーバーヘッドとなり、アプリケーションの要求を満たさないという問題が生じる。これはＤＥＳ以外の暗号アルゴリズムを利用してもソフトウエアで実現する限り同様である。また、実時間処理の条件をクリアするために、動画像処理を専用のハードウエアで行なう場合は、コスト高となるという問題点が生じる。
【０００６】本発明は、上記従来の問題点に鑑み、動画像データのように実時間処理の要求されるデータを扱うアプリケーションに対して、暗号化するに際し、処理コストが低減でき、しかも、実時間処理の制約の中で、十分な機密性の確保、すなわち、正しく復号化して再生する手段を持たない正規以外の利用者による、動画像データの再生を防止できるデータ暗号方式、及びデータ暗号システムを提供することを目的とする。
【０００７】
【課題を解決するための手段】上記目的を達成するために、本発明は、再生順序の規定された複数の再生データの連なりから構成される対象データに対して、機密性保持処理を施すデータ暗号方式であって、前記各再生データの再生順序を規定する再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化する暗号化ステップと、前記再生順序制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生順序制御情報に基づいて再生すべき再生データを決定する復号化ステップとを備えたものである。
【０００８】また再生順序の規定された複数の再生データの連なりから構成される対象データに対して機密性保持処理を施すデータ暗号方式であって、前記各再生データ毎に保持され、次に再生すべき再生データを規定する再生制御情報の一部または全部を暗号化鍵を用いて暗号化する暗号化ステップと、前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生制御情報に基づいて次に再生すべき再生データを決定する復号化ステップととをとを備えたものである。
【０００９】また、再生順序の規定された複数の再生デ

ータの連なりから構成される対象データに対して機密性保持処理を施すデータ暗号方式であって、前記対象データが、再生順序の規定された複数の再生データ群の連なりから構成され、さらに各再生データ群が、それぞれ再生データ群内において再生順序の規定された複数の再生データの連なりから構成される場合に、前記各再生データ群の再生順序を規定する再生順序制御情報と、前記各再生データ毎に保持され、次に再生すべき再生データを規定する再生制御情報と、それぞれ一部または全部を暗号化鍵を用いて暗号化する暗号化ステップと、前記再生順序制御情報と前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、復号化された再生順序制御情報に基づいて再生すべき再生データ群を決定し、復号化された再生制御情報に基づいて再生すべき再生データを決定し、決定された再生データを再生する復号化ステップとをとを備えたものである。

【００１０】また、前記暗号化ステップは、前記再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化し、さらに各再生データを前記再生順序とは無関係な順序に配置して複数の再生データの連なりとする。

【００１１】また、前記暗号化ステップは、前記再生制御情報の一部または全部を暗号化鍵を用いて暗号化し、さらに各再生データを前記再生順序とは無関係な順序に配置して複数の再生データの連なりとする。

【００１２】また前記暗号化ステップは、前記再生順序制御情報と、前記再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化し、さらに前記各再生データ、前記各再生データ群、または前記各再生データと前記各再生データ群を前記再生順序とは無関係な順序に配置して複数の再生データの連なりとする。

【００１３】また前記暗号化ステップは前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化するようにし、前記復号化ステップは暗号化された前記システムストリーム再生順序制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記システムストリーム再生順序制御情報にしたがって、再生すべきシステムストリームを決定する。

【００１４】また前記暗号化ステップは前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリームのGOP 毎に保持され、次に再生するGOP を規定する再生制御情報の一部または全部を暗号化鍵を用いて暗号化するようにし、前記復号化ステップは暗号化された前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記再生制御情報にしたがって、再生すべきGOP を決定する。

【００１５】また前記暗号化ステップは前記対象データが動画像データであり、特にその圧縮方式がMPEG方式に基づいている場合に、前記圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報と、前記圧縮された動画像データのシステムストリームのGOP 毎に保持され、次に再生するGOP を規定する再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化するようにし、前記復号化ステップは暗号化された前記システムストリーム再生順序制御情報と暗号化された前記再生制御情報の暗号化された部分を前記暗号化鍵に対応する復号化鍵を用いて復号化し、この復号化された前記システムストリーム再生順序制御情報にしたがって再生すべきシステムストリームを決定し、復号化された前記再生制御情報にしたがって再生すべきGOP を決定する。

【００１６】また前記暗号化ステップは前記システムストリーム再生順序制御情報の一部または全部を暗号化鍵を用いて暗号化し、前記各システムストリーム群を、再生順序とは無関係な順序に配置する。

【００１７】また前記暗号化ステップは前記再生制御情報の一部または全部を暗号化鍵を用いて暗号化し、前記各GOPを、再生順序とは無関係な順序に配置する。

【００１８】また前記暗号化ステップは前記システムストリーム再生順序制御情報と前記再生制御情報のそれぞれ一部または全部を暗号化鍵を用いて暗号化し、前記各GOP、前記各システムストリーム群、または前記各GOPとシステムストリーム群を再生順序とは無関係な順序に配置する。

【００１９】また前記暗号化ステップに各再生データ間に無意味なデータを配置するステップを追加する。

【００２０】また前記暗号化ステップは前記対象データの一部または全部をも前記暗号化鍵を用いて暗号化するようにし、前記復号化ステップは、前記暗号化された部分をも前記暗号化鍵に対応する復号化鍵を用いて復号化する。

【００２１】また、それぞれデータ入力部より入力されたデータを鍵入力部より入力されたデータを用いて暗号化する第１の暗号アルゴリズム、及び第１の暗号アルゴリズムより高速な第２の暗号アルゴリズムと、前記第１及び第２の暗号化アルゴリズムに、それぞれ対応して、データ入力部より入力されたデータを鍵入力部より入力されたデータを用いて復号化する第１、及び第２の暗号アルゴリズムを用いて前記暗号化ステップにおける暗号化処理は暗号化処理を施すデータを第１、第２、…、第ｎのデータブロックに分割し、前記第１の暗号化アルゴリズムにしたがって、前記データ入力部より入力された前記第１のデータブロックを前記鍵入力部より入力された初期設定値と、暗号化鍵を用いて暗号化し、前記第２

の暗号化アルゴリズムにしたがって、前記データ入力部より入力された前記第ｉ（２≦ｉ≦ｎ）のデータブロックをそれぞれ、前記鍵入力部より入力された前記第（ｉ－１）のデータブロックと、暗号化鍵を用いて暗号化するようにし、前記復号化ステップにおける復号化処理は、前記第１の復号化アルゴリズムにしたがって、前記データ入力部より入力された暗号化された前記第１のデータブロックを前記鍵入力部より入力された、前記初期設定値と前記復号化鍵を用いて復号化し、前記第２の復号化アルゴリズムにしたがって、前記データ入力部より入力された暗号化された、前記第ｉのデータブロックを前記鍵入力部により入力された前記第（ｉ－１）のデータブロックと、前記復号化鍵を用いて復号化し、復号化された前記第１、第２、…、第ｎのデータブロックを結合して前記データを復元する。

【００２２】また前記初期値に変えて、暗号化された第ｊ（ｊは２≦ｊ≦ｎを満たす整数）のデータブロックを用いる。

【００２３】また前記第１の暗号化アルゴリズム及び復号化アルゴリズムは、それぞれ基本処理部をＭ回繰り返す構成とし、前記第２の暗号化アルゴリズム及び復号化アルゴリズムは前記基本処理部をｍ（＜Ｍ）回繰り返す構成とする。

【００２４】

【発明の実施の形態】上記構成により本発明によれば、各再生データの再生順序を規定する再生順序制御情報が暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中で、十分な機密性の確保が保持される。

【００２５】各再生データ毎に保持され、次の再生順序を規定する再生制御情報が暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して実時間処理の制約の中で十分な機密性の確保が保持される。

【００２６】各再生データ群の再生順序を規定する再生順序制御情報と、各再生データ群を構成する各再生データ毎に保持され、次の再生順序を規定する再生制御情報とが暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中で、十分な機密性の確保が保持される。

【００２７】また、再生順序制御情報や、再生制御情報を暗号化鍵を用いて暗号化した上、さらに、各再生データを再生順序とは無関係な順序に配置して複数の再生データの連なりとしたり、または各再生データ群を再生順序とは無関係な順序に配置して複数の再生データ群の連なりとするため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中でより高い安全性が確保される。

【００２８】また、以上のいずれの場合についても実時間処理が要求される再生データ自体は暗号化しないので、ソフトウエア処理も可能であり、処理コストが低減できる。

【００２９】また、対象データが、MPEG方式に基づいている場合には、圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報と、前記圧縮された動画像データのシステムストリームのGOP 単位毎に保持され、次に再生するGOP を規定する再生制御情報の少なくとも一部が暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中で、十分な機密性の確保が保持される。またさらにシステムストリーム群、または前記各GOPを単位として再生順序とは無関係な順序に配置するようにするため、より高い安全性が確保されるとともに、実時間処理が要求される再生データ自体は暗号化しないのでソフトウエア処理も可能であり、処理コストが低減できる。

【００３０】また、暗号化処理を施すデータを第１、第２、…、第ｎのデータブロックに分割し、第１のデータブロックに対しては、暗号化鍵と初期設定値に依存させて、第１の暗号化アルゴリズムで暗号化し、第ｉ（２≦ｉ≦ｎ）のデータブロックに対しては、第（ｉ－１）のデータブロックに依存させて第１の暗号化アルゴリズムより高速な第２の暗号アルゴリズムで暗号化するため、より一層の高速処理が可能となる。

【００３１】また、初期設定値として、暗号化された第ｊ（ｊは２≦ｊ≦ｎの整数）のデータブロックを用いることにより、第１のデータブロックが等しい２つのデータに対して同じ暗号化鍵を用いて暗号化した場合でも、異なる暗号化された第１のデータブロックが得られるため、同じ暗号化鍵を固定的に利用する場合の安全性が向上する。

【００３２】以下、本発明のデータ暗号方式及びデータ暗号システムの一実施例を図面を用いて説明する。

【００３３】なお、本実施例ではMPEG(Motion Picture Expert Group) 方式に基づいて圧縮された動画像データを扱うアプリケーションソフトに対して暗号化する例について説明する。

【００３４】「全体のシステム構成」まず、本実施例における全体のシステム構成について説明する。

【００３５】図１は、本実施例のデータ暗号システムの

概略構成図である。図１に示すようにデータ暗号システムは、ソフト提供者が利用する、暗号化されたアプリケーションを作成するための装置Ａ １と、ソフト利用者が利用する暗号化されたアプリケーションを復号化して再生するための装置Ｂ ２によって構成されている。装置Ａ １は、装置Ａ １全体の動作を制御するCPU ５を有しており、このCPU ５は、バス７を介して、対象データ８と、暗号化アプリケーション作成手段９と、入力手段４と、出力手段６とにそれぞれ接続されている。そして暗号化アプリケーション作成手段は、ＭＰＥＧ符号化手段９Ａと、暗号化手段９Ｂとを備えている。装置Ａ １としては、具体的にはパソコンやワークステーションなどが利用できる。そして装置Ａ １における入力手段より入力された動画像データなどの対象データは、アプリケーション作成手段におけるMPEG符号化手段９Ａで、MPEG符号化され、さらに暗号化手段で暗号化され、出力手段にて配布メディアに適したデータ形式に変換されて出力（記録）される。

【００３６】一方、装置Ｂ ２は、装置Ｂ ２全体の動作を制御するCPU １１を有しており、このCPU １１は、バス１３を介して配付メディア３から受け取った暗号化されたアプリケーション１４と、暗号化アプリケーション再生手段１５と、入力手段１０と出力手段１２に接続されている。暗号化アプリケーション再生手段１５はＭＰＥＧ復号化手段１５Ａと、暗号復号化手段１５Ｂとを備えている。装置Ｂ ２としては、スタンドアローンの再生プレーヤや、パソコンとこれに接続された再生プレーヤなどが利用できる。そして装置Ｂ ２における入力手段より入力された暗号化されたアプリケーションは、暗号化アプリケーション再生手段における暗号復号化手段で復号化され、さらにMPEG復号化手段で、MPEG復号化されて、出力手段にて出力装置に適したデータ形式に変換されて出力される。

【００３７】また、配付メディア３は、ソフト提供者（装置Ａ １）からソフト利用者（装置Ｂ ２）に暗号化されたアプリケーションを配布するためのメディアであり、具体的には、例えば暗号化されたアプリケーションは、CD-ROM、DVD（ディジタルビデオディスク）などに記録されて配布される。

【００３８】「アプリケーションのデータ構造」次に、本実施例で扱うアプリケーションのデータ構造について説明する。

【００３９】図２（ａ）は本実施例で扱うアプリケーションの論理的なデータ構造例である。図２（ａ）に示すように、アプリケーションは、１個以上のセルと、各セルの再生順序を記述したシステムストリーム再生順序制御情報であるプログラムチェーン情報を複数含んでいる。本実施例では、システムストリーム再生順序情報をプログラムチェーン情報（以下PGC情報(ProGramChain)と略記する）と呼ぶ。

【００４０】ここでセルは映画タイトルにおけるシーンや、音楽タイトルにおける曲のように論理的な意味を持つシステムストリームである。各セル、すなわちシステムストリームは、MPEG方式により、ビデオデータ、オーディオデータ、副映像データ、再生制御情報をインタリーブしたものである。ここで、オーディオデータ、副映像データは、例えば英語の音声と日本語の音声、日本語の字幕（副映像）と中国語の字幕などである。

【００４１】またビデオデータは、MPEG方式では、GOP(Group Of Picture)と呼ばれる単位で構成され、GOP は通常１２から１５フレーム、約0.5秒のデータで構成される。そして、ビデオデータの再生制御単位であるGOP毎に、再生制御情報であるデータサーチ情報が保持される。本実施例では、再生制御情報をデータサーチ情報（以下DSI(Data Search Information)情報と略記する）と呼ぶ。

【００４２】図２（ｂ）は、PGC 情報のデータ構造例である。図２（ｂ）に示すように、PGC 情報には、再生制御テーブルを記述し、この中で、各セル毎に、各セルの再生順序を制御するための再生情報（＃１～＃ｎ）を記述する。この再生情報には、例えば、個々のセルデータの開始アドレス（オフセット）や、セルデータのブロック数の情報などを記述する。

【００４３】図２（ｃ）は、DSI 情報のデータ構造例である。図２（ｃ）に示すように、DSI 情報には、次に再生するGOP を制御するためのDSI バックアドレス情報と、カメラアングルアドレス情報などを記述する。そして、このDSI バックアドレス情報には、例えば、早送り再生（ＦＷＤ１、２、…）や、巻き戻し再生（ＢＷＤ１、２、…）などにおける飛び先情報、すなわち、ＦＷＤ１は１コマ送り、ＦＷＤ２は２コマ送り、ＢＷＤ１は１コマ戻り、ＢＷＤ２は２コマ戻りで、それぞれ再生する場合に、次に再生するデータを決定するための情報（DSI情報のアドレス情報）を記述する。また、カメラアングルアドレス情報には、複数のカメラアングル（カメラ位置）の映像データを含む場合に、選択されたカメラアングルに対応して、再生するセルを決定するための情報、すなわちカメラ位置１に対応したセル（アングルセル＃１（ＡＮＧＣ１））や、カメラ位置２に対応したセル（アングルセル＃２（ＡＮＧＣ２））などを決定するための情報（DSI情報のアドレス情報）を記述する。

【００４４】「全体の動作概略」次に、図３は、本実施例におけるアプリケーションの暗号化手段、及び復号化手段におけるデータの全体的な処理の流れを説明するための概念図である。

【００４５】図３に示すように、暗号化手段においては、まず、各セルの再生順序を規定するPGC 情報が暗号化される。PGC 情報が複数ある場合は、それぞれ暗号化する。そして、各セルに対して、ビデオデータの再生単位であるGOP(Group Of Picture）レベルの暗号化処理

を施す。一方復号化手段においては、まず、暗号化された再生順序制御情報が復号化される。そして、各セルに対しては、GOP レベルでの復号化処理を行なう。

【００４６】図４に各セルに対して行うGOP レベルの暗号化処理の流れを示す。図４に示すようにGOP レベルの暗号化処理においては、まず各GOP 毎に付加されるＤＳＩ情報をそれぞれ暗号化する。そして、GOPを単位として、再生順序とは無関係な順序でインタリーブする。

【００４７】図５に各セルに対して行うGOP レベルの復号化処理の流れを示す。図４に示すようにGOP レベルの復号化処理においては、各GOP に付加された暗号化された再生制御情報をそれぞれ復号化する。

【００４８】「鍵の供給方法及び鍵の構成要素」次に、鍵の供給方法について説明する。

【００４９】暗号化手段において、暗号化用の秘密鍵（暗号化鍵）が利用される。この暗号化用秘密鍵としては、１つの秘密鍵を固定的に使用することもできるし、アプリケーション毎に個別の秘密鍵を利用することもできる。前者は秘密鍵が万一露呈したとき、全てのアプリケーションが不正に利用される恐れがあるのに対して、後者はその秘密鍵に対応するアプリケーションのみに被害は限定されるため安全性が高い。

【００５０】次に、この暗号化用秘密鍵の供給方法としては、いくつかの方法を取ることができる。例えば、暗号化手段を実現する暗号モジュールに秘密鍵を組み込んで利用することができる。また、安全性を高めるため、外部提供手段を利用する、すなわち例えば、ICカードなどに秘密鍵を格納し、厳重なアクセス管理の下で利用することもできる。

【００５１】一方、復号化手段１５Ｂにおいて、暗号化用の秘密鍵に対応する復号化用の秘密鍵（復号化鍵）が利用される。この復号化用秘密鍵の装置Ｂ ２への供給方法としてもいくつかの方法を取ることができる。例えば、装置Ｂ ２の復号化手段を実現する復号モジュールに組み込んでおき利用することができる。また、配布メディアであるCD-ROMやDVD のリードイン領域に復号化用秘密鍵を記録し、復号化手段にてそれを読みとって利用することができる。また、安全性を高めるため、外部提供手段を利用する、すなわち、例えば、ICカードなどにおいて、復号化用秘密鍵を格納し、厳重なアクセス管理の下で利用することもできる。

【００５２】なお、CD-ROMやDVD のリードイン領域に復号化用秘密鍵を記録して供給する方法は、通常のファイルシステム単位でのコピーを行なうコピーコマンドでは、リードイン領域はコピーできないため、この意味で安全である。

【００５３】また、復号化用秘密鍵を、暗号化して配布することもできる。この場合は、装置Ｂ ２の復号手段に暗号化された復号用秘密鍵を復号化するための手段を備える必要がある。

【００５４】次に、鍵の構成要素について説明する。暗号化手段において利用される暗号化用の秘密鍵の構成要素としては以下で述べるセルレベルでの暗号化に利用する秘密鍵Ｋ１と、GOP レベルでの暗号化に利用する秘密鍵Ｋ２がある。また復号化手段において利用される復号化用の秘密鍵の構成要素としては、セルレベルでの復号化に利用する秘密鍵Ｋ１’と、GOP レベルでの復号化に利用する秘密鍵Ｋ２’とがある。

【００５５】ただし、セルレベルに利用する秘密鍵Ｋ１と、GOP レベルで利用する秘密鍵Ｋ２は同じものを利用してもよい。また、前述のように全てのアプリケーションに固定であっても、アプリケーション毎に個別であっても構わない。

【００５６】以下、簡単のためセルレベルに利用する秘密鍵Ｋ１と、GOP レベルで利用する秘密鍵Ｋ２は同じもの、すなわち秘密鍵Ｋとして説明する。復号化に利用するのは秘密鍵Ｋ’である。

【００５７】「詳細な動作」次に本実施例の動作（１）から（３）を詳細に説明する。

（１）本実施例全体の処理の流れ

図６は、本実施例の全体の処理の流れを示すフローチャートである。図６に示すように、まず装置Ａ １において暗号化アプリケーションの作成処理を行なう（ステップＳ１０１）。その後、装置Ａ １から装置Ｂ ２へ暗号化アプリケーションの配付処理を行なう（ステップＳ１０２）。そして、装置Ｂ ２において、暗号化されたアプリケーションの再生処理を行なう（ステップＳ１０３）。

（２）装置Ａ １におけるアプリケーションの暗号化処理の流れ（前記ステップＳ１０１）

図７は、暗号化アプリケーションの作成処理（前記ステップＳ１０１）の流れを示すフローチャートである。図７に示すように、まず、対象データの入力処理の後（ステップＳ２０１）、セルレベルの暗号化処理が施され（ステップＳ２０２）、次にＧＯＰレベルの暗号化処理が施され（ステップＳ２０３）、暗号化されたアプリケーションの出力処理が施される（ステップＳ２０４）。

【００５８】図８、及び図９は、それぞれ、セルレベルの暗号化処理（前記ステップＳ２０２）の流れ、及びＧＯＰレベルの暗号化処理（前記ステップＳ２０３）の流れを示すフローチャートである。

【００５９】まず、セルレベルの暗号化処理（前記ステップＳ２０２）は、図８に示すように、まず、PGC 情報かどうかを判定し（ステップＳ３０１）、PGC 情報であれば、それを秘密鍵Ｋを用いて暗号化する（ステップＳ３０２）。そして、ステップＳ３０１、及びＳ３０２の処理を全てのPGC 情報に対して繰り返し施す（ステップＳ３０３）。

【００６０】ここで、PGC情報の暗号化は、例えば、図２（ｂ）に示すＰＧＣ情報における、個々のセルデータ

へのアドレス（オフセット）と、セルデータのブロック数の情報のみを暗号化対象とすることができる。

【００６１】一方、GOP レベルの暗号化処理（前記ステップＳ２０３）は、図９に示すように、 まずセルかどうか判定し（ステップＳ４０１）、セルであれば、次にDSI情報かどうかを判定し（ステップＳ４０２）、DSI情報であれば、それを秘密鍵Ｋを用いて暗号化する（ステップＳ４０３）、そしてステップＳ４０２、Ｓ４０３の処理を、該当のセルにおける全てのＤＳＩ情報に対して繰り返し施す（ステップＳ４０４）。そして、該当のセルにおいて、GOP を単位として、再生順序とは無関係な順序にインタリーブ（配置変換）する（ステップＳ４０５）。そして、以上ステップＳ４０１からＳ４０５の処理を全てのセルに対して繰り返し施す（ステップＳ４０６）。

（３）装置Ｂ ２におけるアプリケーションの暗号化処理の流れ（前記ステップＳ１０２）

図１０は、アプリケーションの復号化処理（前記ステップＳ１０２）の流れを示すフローチャートである。図１０に示すように、まず暗号化アプリケーションの入力処理の後（ステップＳ５０１）、セルレベルの復号化処理が施され（ステップＳ５０２）、次にＧＯＰレベルの復号化処理が施され（ステップＳ５０３）、復号化されたアプリケーションの出力処理が施される（ステップＳ５０４）。

【００６２】図１１、及び図１２は、それぞれセルレベルの復号化処理（前記ステップＳ５０２）の流れ、及びＧＯＰレベルの復号化処理（前記ステップＳ５０３）の流れを示すフローチャートである。

【００６３】まず、セルレベルの復号化処理（前記ステップＳ５０２）は、図１１に示すように、まず暗号化されたPGC 情報かどうかを判定し（ステップＳ６０１）、暗号化されたPGC 情報であれば、それを前記秘密鍵Ｋに対応するの秘密鍵Ｋ’を用いて復号化する（ステップＳ６０２）。そして、ステップＳ６０１、及びＳ６０２の処理を、全ての暗号化されたPGC 情報に対して繰り返し施す（ステップＳ６０３）。

【００６４】一方、GOP レベルの復号化処理（前記ステップＳ５０３）は、図１２に示すように、 まず、セルかどうか判定し（ステップＳ７０１）、セルであれば、該当のセルにおいて、暗号化されたDSI 情報かどうかを判定し（ステップＳ７０２）、暗号化されたDSI 情報であれば、それを秘密鍵Ｋ’を用いて復号化する（ステップＳ７０３）、そしてステップＳ７０２、Ｓ７０３の処理を、該当のセルにおける全てのＤＳＩ情報に対して繰り返し施す（ステップＳ７０４）。そして、以上ステップＳ７０１からＳ７０４の処理を、全てのセルに対して繰り返し施す（ステップＳ７０５）。

【００６５】「安全性」本実施例では、再生されるデータ（GOP）自体は暗号化されないが、GOP の再生を制御するDSI 情報や、GOP群 を含むセルの再生順序を規定するPGC 情報が暗号化される上、GOP単位で再生順序とは無関係な順序でインタリーブしている。このため、復号化用の秘密鍵の供給を受けていない正規以外の利用者（攻撃者）が、例えば図２１に示すように、MPEG復号手段を備えた汎用パソコンに、再生プレーヤおよびハードディスクを接続し、上述の処理により暗号化されたアプリケーションを再生しようとしても、暗号化された部分を復号化する暗号復号化手段がないので正しく再生できない。また、一旦ハードディスクにファイル単位で記録して再生しようとしても、やはり復号化手段を持たないでの正しい順序で再生できない（例えば各GOP は通常約0.5秒のデータからなるため、約0.5秒毎にランダムに変化する映像データが再生されるだけである。）。

【００６６】なお、復号化用の秘密鍵の供給方法として、前述したように、CD-ROMやDVD のリードイン領域に復号化用秘密鍵を記録する方法をとることもできる。この場合は、通常の、ファイルシステム単位でのコピーを行なうコピーコマンドでは、リードイン領域はコピーできないため、この意味で安全である。なお、リードイン領域の読みとりが可能な、低レベルディスクアクセス手段を有するより強力な攻撃者に対しては、この場合機密性が確保されないが、それは本実施例の対象外とする。

【００６７】以上の構成により、動画像データのように時系列に再生され、しかも実時間処理の要求されるデータを扱うアプリケーションに対して、データを暗号化するに際し、ソフトウエア処理が可能なため処理コストが低減でき、しかも、実時間処理の制約の中で十分な機密性の確保ができる。

【００６８】以上の実施例における、PGC情報や、DSI情報の暗号化及び復号化に利用する暗号モジュールとしては、例えば、DESなどに代表される秘密鍵暗号や、疑似乱数生成器を用いたストリーム暗号を利用することができる。

【００６９】なお、本発明は、以上説明した実施例に限定されず種々の変形が可能である。その例としては例えば次のものがある。

（１）本実施例では、セルレベルの暗号化処理（PGC情報の暗号化処理）と、GOPレベルの暗号化処理（DSI情報の暗号化及びGOP単位のランダムなインタリーブ処理）とを両方施す構成としたが、いずれか一方のみ施す構成とすることが可能である。また、インタリーブ処理の単位をGOP 単位としてが、それには限定されない。

（２）本実施例では、PGC情報や、DSI情報の暗号化処理及び復号化処理に利用する暗号モジュールとしては特に限定せず、例えば、DESなどに代表される秘密鍵暗号や、疑似乱数生成器を用いたストリーム暗号を利用することができるとした。

【００７０】しかしながら、さらに高速に処理するために、DES など代表される秘密鍵暗号を以下に述べるブロ

ック連鎖法を利用することができる。

【００７１】図１５、図１６はブロック連鎖法における暗号化処理及び復号化処理における秘密鍵暗号の利用手順を示す構成図である。また図１３、図１４は、それぞれブロック連鎖法における暗号化処理、及び復号化処理におけるデータの流れを示すフローチャートである。

【００７２】図１５に示すように、暗号化処理の対象データは、まず、データブロック（Ｐ１、Ｐ２、…，Ｐｎ）に分割される。データブロックのサイズは、暗号化関数Ｅ１、Ｅ２の入力サイズであり、ｎは適当に定めるものとする。そして、対象データがｎブロック以上である場合は、以下の処理を、ｎ個のデータブロック毎に繰り返す。

【００７３】そして、図１５に示すように、Ｐ１は、秘密鍵Ｋ、及び初期設定値ＩＶに依存させて、暗号化関数Ｅ１を用いて暗号化し、Ｐｉ（２≦ｉ≦ｎ）は、秘密鍵Ｋ、及びＰｉ－１に依存させて、暗号化関数Ｅ２を用いて、順次暗号化し、暗号化されたデータブロック（Ｃ１、Ｃ２、…，Ｃｎ）を生成する。

【００７４】一方、復号化処理は図１６に示すように、暗号化されたデータブロック（Ｃ１、Ｃ２、…，Ｃｎ）に対して、まずＣ１が、秘密鍵Ｋおよび初期設定値ＩＶに依存させて、復号化関数Ｄ１を用いて復号化し、Ｃｉ（２≦ｉ≦ｎ）は、秘密鍵Ｋ、及びＰｉ－１に依存させて、復号化関数Ｄ２を用いて、順次復号化し、復号化されたデータブロック（Ｐ１、Ｐ２、…，Ｐｎ）を生成する。

【００７５】そして、暗号化関数Ｅ１としては、例えばＤＥＳ暗号、暗号化関数Ｅ２としては、ＤＥＳ暗号より高速処理可能な簡易暗号（例えば、Ｐｉ－１をシードとして発生させた乱数をＰｉに加算するなど）を利用することができる。

【００７６】この場合、処理速度についてはＤＥＳを繰り返し利用するよりも高速化されるのはいうまでもない。また安全性については、ここでは、秘密鍵Ｋをしらない攻撃者が、暗号化されたデータブロック（Ｃ１、Ｃ２、…，Ｃｎ）から元のデータブロック（Ｐ１、Ｐ２、…，Ｐｎ）を解読できるかについて説明する。

【００７７】この場合、Ｃｉ（２≦ｉ≦ｎ）を解読するためには、Ｐｉ－１を解読する必要があることから、結局、Ｐ１が解読されれば、順次、Ｐ２、Ｐ３、…が解読することができる。しかし、Ｐ１の解読については、ＤＥＳ暗号が利用されているため、暗号文のみから解読するのは不可能と考えられる。

【００７８】したがってこのような構成により、安全性はについては、暗号文のみによる攻撃に関する限り低下することなく、高速処理が可能となるという効果が得られる。

【００７９】また、初期値として、２番目以降の暗号化されたデータブロック（Ｃ２、…，Ｃｎ）の中の１つを利用することができる。この構成により、異なる２つのデータに対して同じ鍵Ｋ及び初期値で暗号化する場合で、１番目のデータブロックＰ１がたまたま一致している場合でも、その出力であるＣ１は異ならせることができ、安全性を高めることができる。図１９、図２０に、Ｃ２を初期設定値として利用する場合の暗号化処理、および復号化処理の構成を、図１７、図１８に暗号化処理、および復号化処理の流れを示すフローチャートを示す。

【００８０】また、上述の例では、初期値ＩＶ、および、Ｐｉ－１によって変換された秘密鍵Ｋを鍵入力部より入力する構成としたが、初期値ＩＶ、および、Ｐｉ－１によってＰｉを変換し、データ入力部より入力する構成も可能である。

【００８１】また、暗号化関数Ｅ１を基本処理部をＭ回繰り返す暗号とし、また、暗号化関数Ｅ２を基本処理部をｍ（＜Ｍ）回を繰り返す暗号とすることができる。

【００８２】この場合、Ｅ１およびＥ２の基本処理部は同一なので、それらを共有でき、それぞれ別の暗号にする場合に比べて暗号モジュールの容量をコンパクトにすることができる。

（３）GOP レベルの暗号化処理、復号化処理における暗号化とインタリーブ、及び復号化とデインタリーブの各処理の順序は、上述の実施例の順序に制限されものではない。例えば、暗号化処理において、インタリーブ後、暗号化したものを、復号処理において、復号化した後、デインタリーブしてもいい。また、インタリーブ後、暗号化したものを上述の実施例の順序で復号処理してもいいし、上述の実施例の順序で暗号処理したものを復号化した後、デインタリーブしてもよい。

（４）本実施例では、データは暗号化しなかったが、実時間処理制約の中で可能であれば、データの少なくとも一部を暗号化しても構わない。

（５）本実施例では、MPEG仕様に基づいアプリケーションの場合について説明したが、その他の仕様に基づいたアプリケーションに対しても適用可能である。

（６）本実施例では、アプリケーションの配布メディアとして、CD-ROM、DVDとしたが、その他の記録メディアや、衛星やCATVなどの各種通信網を利用した放送、通信メディアを配布メディアとして利用することができる。

【００８３】

【発明の効果】各再生データの再生順序を規定する再生順序制御情報が暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中で十分な機密性の確保が保持される。

【００８４】各再生データ毎に保持され、次の再生順序を規定する再生制御情報が暗号化鍵を用いて暗号化され

るため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して実時間処理の制約の中で、十分な機密性の確保が保持される。

【００８５】各再生データ群の再生順序を規定する再生順序制御情報と、各再生データ群を構成する各再生データ毎に保持され、次の再生順序を規定する再生制御情報と、が暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して実時間処理の制約の中で、十分な機密性の確保が保持される。

【００８６】また、再生順序制御情報や、再生制御情報を、暗号化鍵を用いて暗号化した上、さらに、各再生データを再生順序とは無関係な順序に配置して複数の再生データの連なりとしたり、または、各再生データ群を再生順序とは無関係な順序に配置して複数の再生データ群の連なりとするため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が、各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中でより高い安全性が確保される。

【００８７】また、以上のいずれの場合についても、実時間処理が要求される再生データ自体は、暗号化しないので、ソフトウエア処理も可能であり、処理コストが低減できる。

【００８８】また、対象データが、MPEG方式に基づいている場合には、圧縮された動画像データのシステムストリーム群の再生順序を規定するシステムストリーム再生順序制御情報と、前記圧縮された動画像データのシステムストリームのGOP 単位毎に保持され、次に再生するGOP を規定する再生制御情報の少なくとも一部が暗号化鍵を用いて暗号化されるため、この暗号化鍵対応する復号化鍵を有しない正規以外の利用者が各再生データを正しい順序で再生することは不可能であり、再生データの連なりである対象データに対して、実時間処理の制約の中で、十分な機密性の確保が保持される。また、さらにシステムストリーム群、または、前記各GOPを単位として再生順序とは無関係な順序に配置するようにするため、より高い安全性が確保されるとともに、実時間処理が要求される再生データ自体は、暗号化しないので、ソフトウエア処理も可能であり、処理コストが低減できる。

【００８９】また、暗号化処理を施すデータを第１、第２、…、第ｎのデータブロックに分割し、第１のデータブロックに対しては、暗号化鍵と初期設定値に依存させて、第１の暗号化アルゴリズムで暗号化し、第ｉ（２≦ｉ≦ｎ）のデータブロックに対しては、暗号化鍵と、第（ｉ－１）のデータブロックに依存させて、第１の暗号化アルゴリズムより高速な第２の暗号アルゴリズムで暗号化するため、より一層の高速処理が可能となる。

【００９０】また、初期設定値として、暗号化された第ｊ（ｊは２≦ｊ≦ｎの整数）のデータブロックを用いることにより、第１のデータブロックが等しい２つのデータに対して、同じ暗号化鍵を用いて暗号化した場合でも、異なる暗号化された第１のデータブロックが得られるため、同じ暗号化鍵を固定的に利用する場合の安全性が向上する。

【図面の簡単な説明】

【図１】本発明の一実施例におけるデータ暗号システムの構成図

【図２】（ａ）は本発明の一実施例におけるアプリケーションの論理的なデータ構造図

（ｂ）は本発明の一実施例におけるＰＧＣ情報のデータ構造を示す図

（ｃ）は本発明の一実施例におけるＤＳＩ情報のデータ構造を示す図

【図３】本発明の一実施例における暗号化、復号化のデータ処理を示す図

【図４】本発明の一実施例におけるＧＯＰレベルの暗号化処理を示す図

【図５】本発明の一実施例におけるＧＯＰレベルの復号化処理を示す図

【図６】本発明の一実施例におけるシステム全体の処理のフローチャート

【図７】本発明の一実施例における暗号化アプリケーション作成処理のフローチャート

【図８】本発明の一実施例におけるセルレベルの暗号化処理のフローチャート

【図９】本発明の一実施例におけるＧＯＰレベルの暗号化処理のフローチャート

【図１０】本発明の一実施例における暗号化アプリケーション再生処理のフローチャート

【図１１】本発明の一実施例におけるセルレベルの復号化処理のフローチャート

【図１２】本発明の一実施例におけるＧＯＰレベルの復号化処理のフローチャート

【図１３】本発明の一実施例におけるブロック連鎖法を用いた暗号化処理のフローチャート

【図１４】本発明の一実施例におけるブロック連鎖法を用いた復号化処理のフローチャート

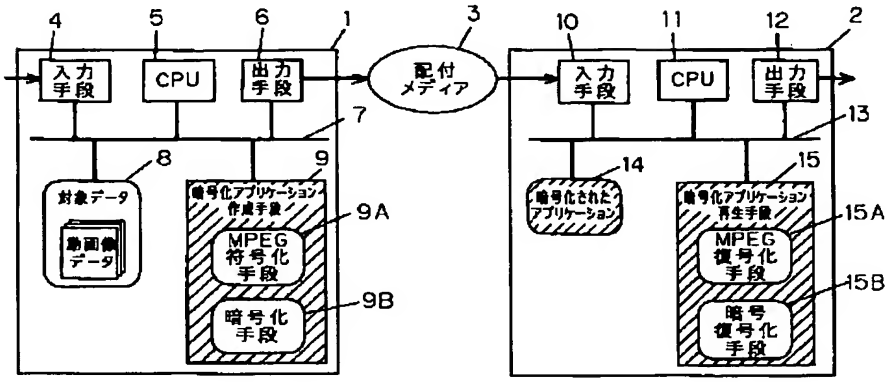
【図１５】本発明の一実施例におけるブロック連鎖法を用いた暗号化処理での秘密鍵暗号の利用手順を示す構成図

【図１６】本発明の一実施例におけるブロック連鎖法を用いた復号化処理での秘密鍵暗号の利用手順を示す構成図

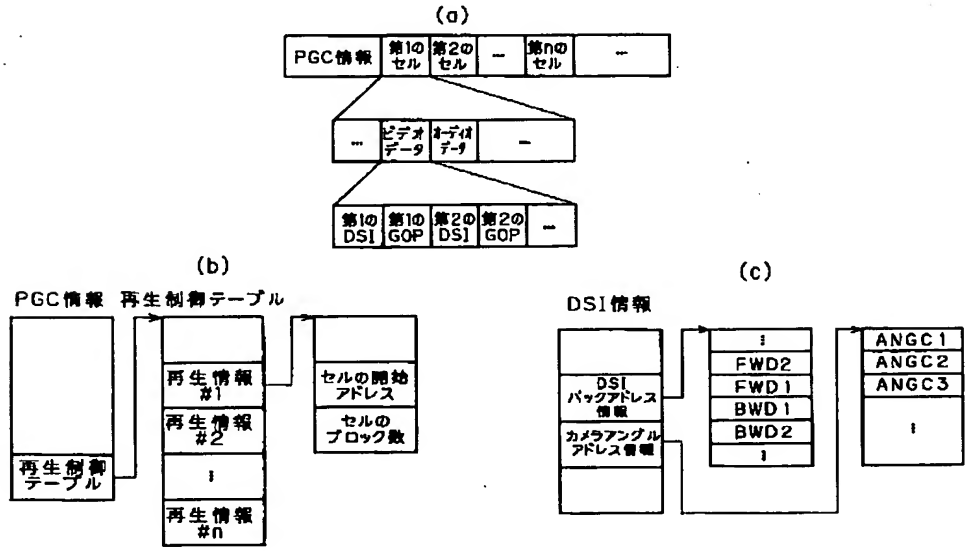
【図１７】本発明の一実施例におけるＣ２を初期設定値として利用する場合のブロック連鎖法を用いた暗号化処

理のフローチャート
【図１８】本発明の一実施例におけるＣ２を初期設定値として利用する場合のブロック連鎖法を用いた復号化処理のフローチャート
【図１９】本発明の一実施例におけるＣ２を初期設定値として利用する場合のブロック連鎖法を用いた暗号化処理の構成図
【図２０】本発明の一実施例におけるＣ２を初期設定値として利用する場合のブロック連鎖法を用いた復号化処理の構成図
【図２１】本発明の一実施例における利用者側のシステム構成例を示す図
【符号の説明】
１　装置Ａ
２　装置Ｂ
３　配付メディア
４　入力手段
５　ＣＰＵ
６　出力手段
７　バス
８　対象データ
９　暗号アプリケーション作成手段
１０　入力手段
１１　ＣＰＵ
１２　出力手段
１３　バス
１４　暗号化されたアプリケーション
１５　暗号化されたアプリケーション再生手段

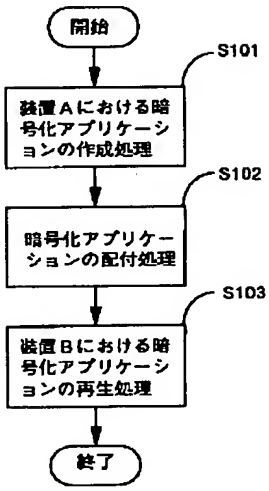
【図１】



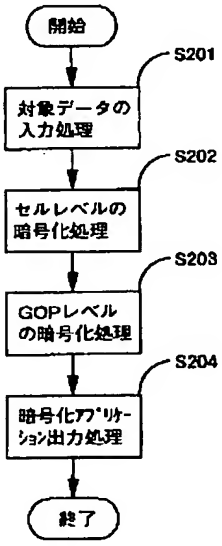
【図２】



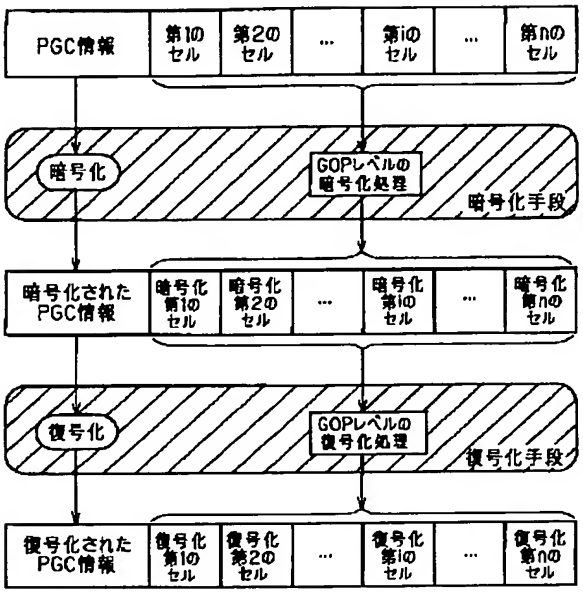
【図６】



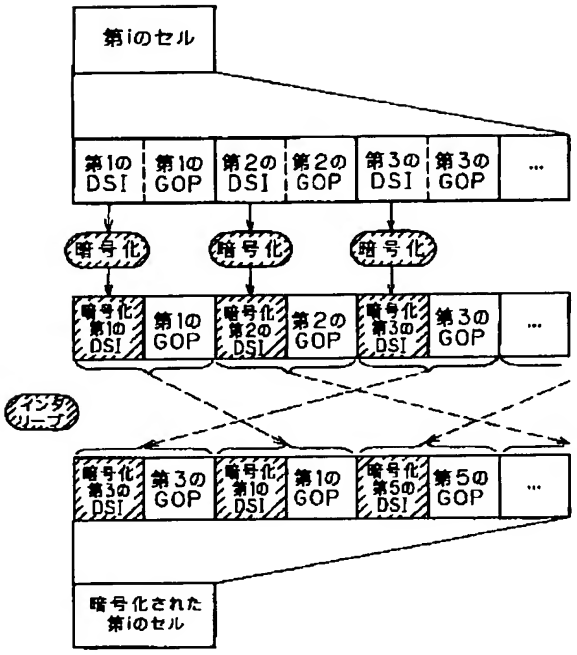
【図７】



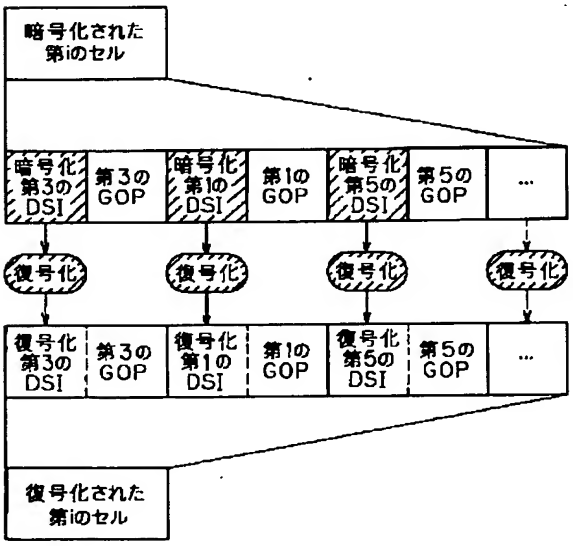
【図３】



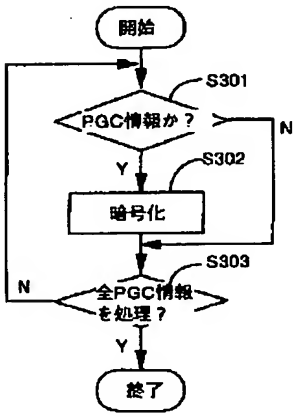
【図４】



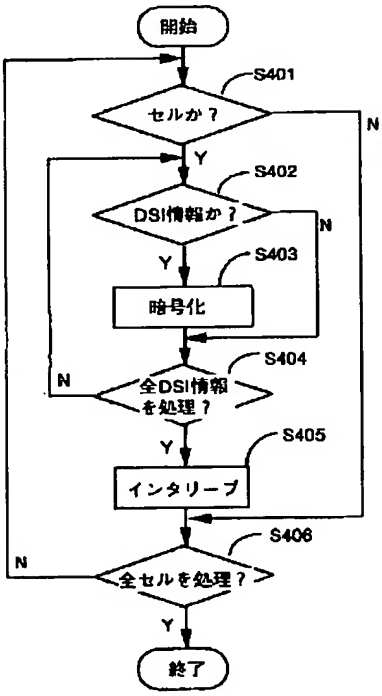
【図５】



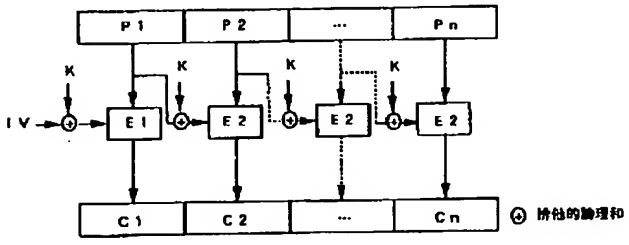
【図８】



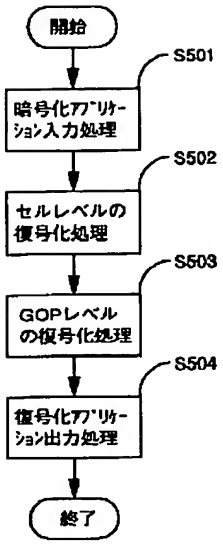
【図９】



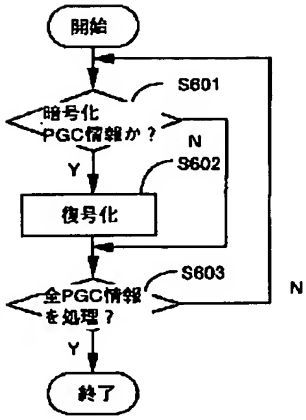
【図１５】



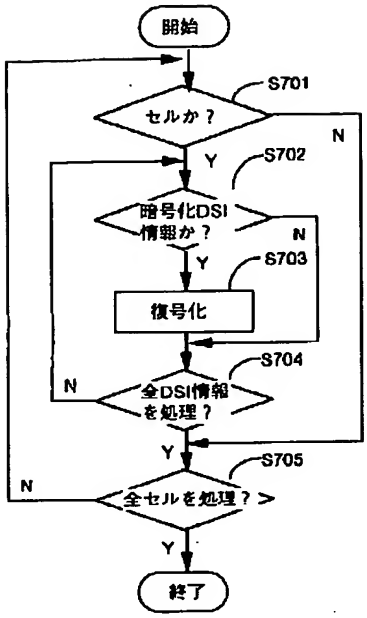
【図１０】



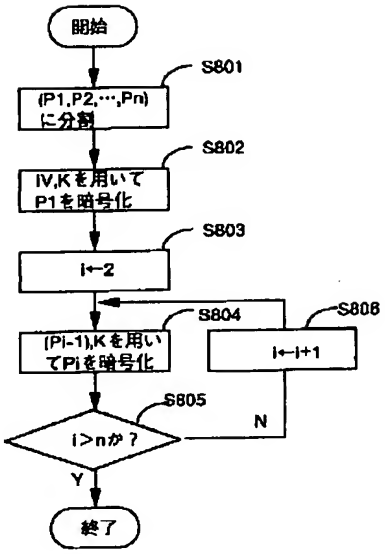
【図１１】



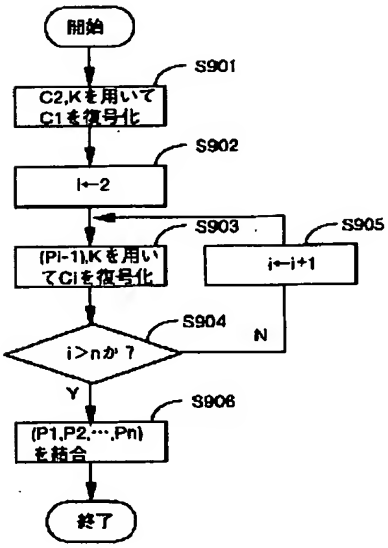
【図１２】



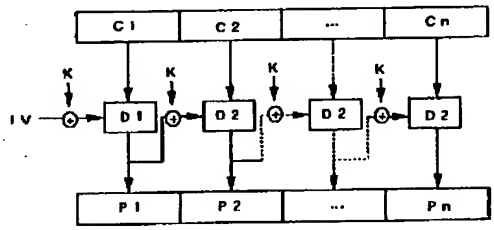
【図１３】



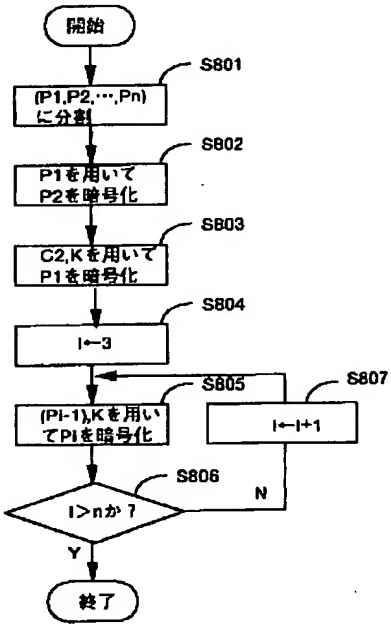
【図１４】



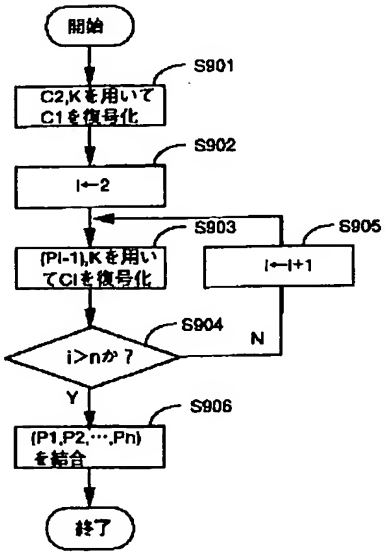
【図１６】



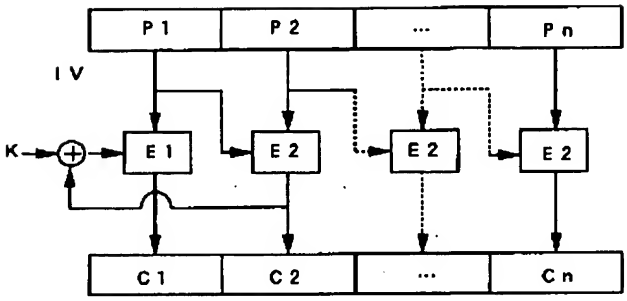
【図１７】



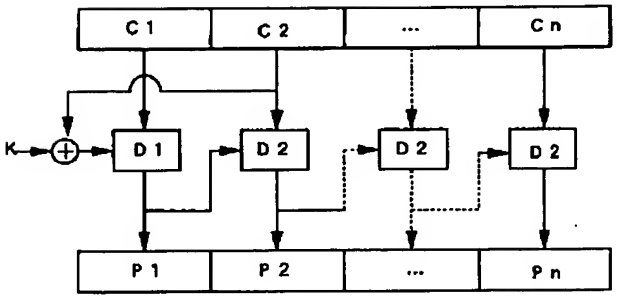
【図１８】



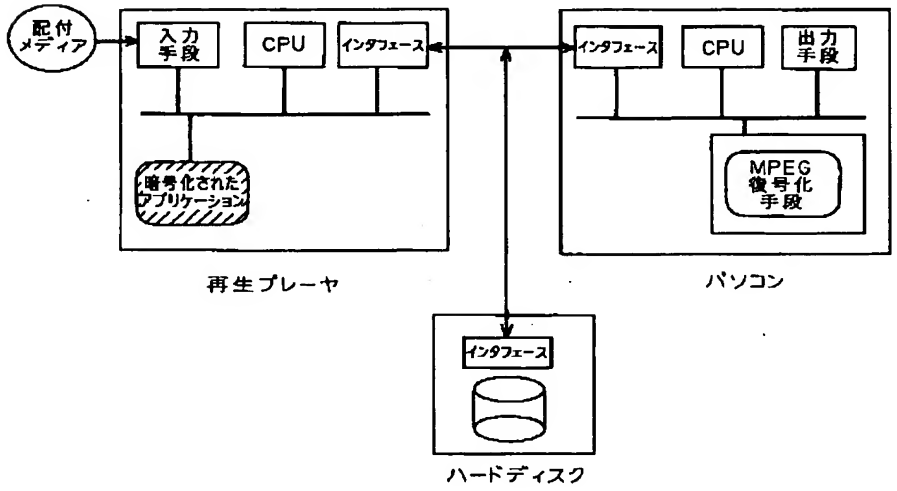
【図１９】



【図２０】



【図２１】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
Ｈ０４Ｌ　9/34			Ｈ０４Ｌ　9/00	６８１	

(72)発明者　小塚　雅之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　山内　一彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内